# Negative Evidence

## Negative Definitions

### Privacy

#### Privacy is an individual right

Nikki Gulzar, Basra Abbasi, Eddie Wu, Anil Ozbal, & WeiQi Yan, 2013 [Auckland University of Technology], “Surveillance Privacy Protection” <http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf>

Whenever we are under surveillance, privacy becomes an issue. Privacy has been commonly used within western society, however, it was not a general concept and to many cultures it was virtually unknown, until recently [95]. Privacy is an individual right to control what happens with personal data [71, 102]. The meaning of privacy may differ throughout cultures but the general conception is that privacy means wanting to keep information unnoticed or unidentified from the general public. Privacy can be categorized in different contexts [35, 65].

#### Privacy includes any information available about an individual

Waldo, James; **Lin**, Herbert S.; and Cox, Lawrence H. (2010) "Thinking About Privacy: Chapter 1 of "Engaging Privacy and Information Technology in a Digital Age"," Journal of Privacy and Confidentiality: Vol. 2: Iss. 1, Article 4. Available at: <http://repository.cmu.edu/jpc/vol2/iss1/4>

The committee began by trying to understand what privacy is, and it quickly found that privacy is an ill-defined but apparently well-understood concept. It is ill-defined in the sense that people use the term to mean many different things. Any review of the literature on privacy will reveal that privacy is a complicated concept that is difficult to define at a theoretical level under any single, logically consistent “umbrella” theory, even if there are tenuous threads connecting the diverse meanings. Specifying the concept in a way that meets with universal consensus is a difficult if not impossible task, as the committee found in doing its work. At the same time, the term “privacy” is apparently well understood in the sense that most people using the term believe that others share their particular definition. Nonetheless, privacy resists a clear, concise definition because it is experienced in a variety of social contexts. For example, a question may be an offensive privacy violation in one context and a welcome intimacy in another. The committee believes that in everyday usage, the term “privacy” generally includes reference to the types of information available about an individual, whether they are primary or derived from analysis. These types of information include behavioral, financial, medical, biometric, consumer, and biographical. Privacy interests also attach to the gathering, control, protection, and use of information about individuals. Informational dimensions of privacy thus constitute a definitional center of gravity for the term that is used in this report, even while recognizing that the term may in any given instance entail other dimensions as well—other dimensions that are recognized explicitly in the discussion.2

#### Physical privacy prevents intrusion into an individual’s life

Nikki Gulzar, Basra Abbasi, Eddie Wu, Anil Ozbal, & WeiQi Yan, 2013 [Auckland University of Technology], “Surveillance Privacy Protection” <http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf>

Personal privacy is one of the first issues that are being violated. Personal privacy allows an individual to keep their body or beliefs private. Physical privacy can be defined as preventing intrusion into one’s personal space or solitude. The concerns may be [59]: Not allowing personal possessions searched by an unwelcome party. Not allowing access to people’s homes and vehicle without authorization. Most countries have trespassing and property rights which help to determine the right to physical properties [44].

#### Data Privacy is an evolving area

Nikki Gulzar, Basra Abbasi, Eddie Wu, Anil Ozbal, & WeiQi Yan, 2013 [Auckland University of Technology], “Surveillance Privacy Protection” <http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf>

Data privacy is the second most important issue when it comes to privacy. We all want to secure our personal data but data privacy is about an evolving relationship between technology and legal rights, which makes it harder to keep data private. The data storage causes some privacy issues such as who will access to the data, how the data is stored and the user’s rights for protection [67]. There are some web sites that ask for more data than necessary but it is unclear as to what they share. Privacy issues especially to personal data include insecure, electronic transmission, data trails and logs of email messages, and the tracking of web pages visited [102]. Nowadays every kind of organization is marketing online users, which means that we are putting more of our personal data online and sometimes it becomes hard to keep track of all the information. Without our knowledge, the data could be sold to make profits [39, 47]. Therefore data privacy has become very important, it gives us a little control over the information we share, and the penalty for privacy violation has become more severe.

#### Organizational Privacy is Internet Privacy

Nikki Gulzar, Basra Abbasi, Eddie Wu, Anil Ozbal, & WeiQi Yan, 2013 [Auckland University of Technology], “Surveillance Privacy Protection” <http://staff.elena.aut.ac.nz/Wei-Yan/VC/articles/SPP.pdf>

Organizational privacy allows government agencies or organizations to keep their activities private and prevent it from being leaked to other organizations. Each organization has its own privacy policy, which helps them to maintain the privacy of personal data. An example of the organizational privacy is internet privacy. When organizations have web interactions for their customers, they must take customers’ right into consideration when it comes to their personal data [26]. Data Privacy Day is about empowering people to protect their privacy and control their digital foot- prints to ensure the protection of data privacy [4].

## Abuse of Power

#### Activities are too shrouded in secrecy and Abuse Occurs because of it

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or- imagined

You say you are unaware of a single instance, since 9/11, in which the government used surveillance to target a political opponent, dissenter or critic. But if the government were using surveillance this way, would officials tell us? So much secrecy surrounds the government’s surveillance activities that we simply don’t know how often, or in what ways, the government’s surveillance powers have been abused. This said, we know enough that we ought to be worried. Here is an article about the Department of Homeland Security conducting inappropriate surveillance of protesters associated with Occupy Wall Street. Here is a report of the Justice Department’s inspector general finding that the F.B.I. monitored a political group because of its anti-war views. Here is a story in which a former C.I.A. official says that the agency gathered information about a prominent war critic “in order to discredit him.”’

#### Opportunities for abuse and blackmail are endless

Goldberg, Jonah. [contributing editor to National Review, named by the Atlantic magazine as one of the top 50 political commentators in America]. "Civil libertarians' hypocrisy," American Enterprise Institute. July 8, 2013, <http://aei.org/article/politics-and-public-opinion/civil-libertarians-> hypocrisy/

"At least 850,000 people have security clearances that give them access to this information," Tiffiniy Cheng of Fight for the Future recently wrote on The Huffington Post. "That's the size of Boston. Imagine if they leak information about a politician or business leaders' personal life — what about a prominent activist? The opportunities for abuse and blackmail are endless; despite what some members of Congress have claimed, the history of government surveillance programs is riddled with abuses." Farhad Manjoo of online Slate magazine agrees. The "fundamental problem" with the NSA's surveillance program is that it's amassing an all-too-tempting stockpile of information. "Someone has access to that data, and that someone might not be as noble as (Edward) Snowden. He could post everything online. He could sell it to identity thieves. He could blackmail you. Or he might blackmail politicians, businesspeople, judges, TSA agents, or use the data in some other nefarious way." One needn't be a privacy absolutist, never mind a paranoid conspiracy theorist, to believe that this is a legitimate concern. One can even support the NSA's PRISM program and still want significant safeguards against abuse.

## Civil Liberties, Democracy, and Freedom

#### NSA Surveillance threaten the basis of democracy

Peter M. Shane, [Chair in Law, Moritz College of Law, Ohio State University], "Foreword: The NSA And the Legal Regime for Foreign Intelligence Surveillance," A Journal of Law and Policy for the Information Society, 2014.

For civil libertarians, however, any such argument is quite likely to pale given the more direct civil liberties impacts of mass surveillance. In NSA Surveillance: The Implications for Civil Liberties, Shayana Kadidal, the senior managing attorney of the Guantánamo Global Justice Initiative at the Center for Constitutional Rights in New York City, asserts that such programs threaten the very independence of citizen thought and action that are central to democratic governance.144 He illustrates that idea concretely by explaining the impact of the NSA programs on his own work and on the work of other lawyers who represent politically unpopular or vulnerable clients. Like Professors Mueller and Stewart, he also calls into question the “liberty-security tradeoff” meme. Like them, he calls into question the few successes publicly identified with the NSA programs and worries, as they do, that the extraordinary rate of false positives means that the FBI is too often spending significant time and effort on leads that go nowhere.145

#### Liberal Democracy CANNOT exist without Privacy

David Cole, [Georgetown University Law Center], "Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism," in Surveillance, Counter-Terrorism, and Comparative Constitutionalism, New York: Routledge 2013.

In 1956, at the height of McCarthyism in the US, sociologist Edward Shils wrote that liberal democracy demands confidentiality for its citizens and transparency for its government.8 Today, it is the citizenry that is increasingly transparent, while government operations are shrouded in secrecy. That development poses a serious challenge not merely to privacy but to liberty and democracy. Sir Thomas Erskine May's words from 1863 apply with equal if not greater immediacy 150 years later: Next in importance to personal freedom is immunity from suspicions and jealous observation. Men may be without restraints upon their liberty; they may pass to and fro at pleasure; but if their steps are tracked by spies and informers, their words noted down for crimination, their associates watched as conspirators - who shall say that they are free? Nothing is more revolting to Englishmen than the espionage which forms part of the administrative system of continental despotisms. It haunts men like an evil genius, chills their gaiety, restrains their wit, casts a shadow over their friendships, and blights their domestic hearth. The freedom of this country may be measured by its immunity from this baleful agency.9

#### Surveillance threatens basic privacy and democratic participation, threatening all of society

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Privacy Is Worth Protecting," The New York Times. June 9, 2013, http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or- imagined

These abuses are real, but if we focus on them exclusively we risk overlooking the deeper implications of pervasive government surveillance. When people think the government is watching them, or that it might be, they become reluctant to exercise democratic freedoms. They may be discouraged from visiting officially disfavored Web sites, joining controversial political groups, attending political rallies or criticizing government policy. This is a cost to the people who don’t exercise their rights, but it’s a cost to our society, too. The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital. This is the greater threat presented by the kinds of programs that were exposed this past week.

#### The Surveillance State is the Death Knell for Democracy

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), http://www.harvardlawreview.org/media/pdf/vol126\_cohen.pdf

If, as I have argued, the capacity for critical subjectivity shrinks in conditions of diminished privacy, what happens to the capacity for democratic self-government? Conditions of diminished privacy shrink the latter capacity as well, because they impair the practice of citizenship. But a liberal democratic society cannot sustain itself without citizens who possess the capacity for democratic self-government. A society that permits the unchecked ascendancy of surveillance infrastructures cannot hope to remain a liberal democracy. Under such conditions, liberal democracy as a form of government is replaced, gradually but surely, by a different form of government that I will call modulated democracy because it relies on a form of surveillance that operates by modulation. Modulation and modulated democracy are emerging as networked surveillance technologies take root within democratic societies characterized by advanced systems of informational capitalism. Citizens within modulated democracies — citizens who are subject to pervasively distributed surveillance and modulation by powerful commercial and political interests — increasingly will lack the ability to form and pursue meaningful agendas for human flourishing.

#### Diminished Privacy Stifles Innovation

Cohen, Julie. [Law Professor at Georgetown University]. "WHAT PRIVACY IS FOR," 126 Harvard Law Review. 1904 (2013), http://www.harvardlawreview.org/media/pdf/vol126\_cohen.pdf

Conditions of diminished privacy also impair the capacity to innovate. This is so both because innovation requires the capacity for critical perspective on one’s environment and because innovation is not only about independence of mind. Innovation also requires room to tinker, and therefore thrives most fully in an environment that values and preserves spaces for tinkering. A society that permits the unchecked ascendancy of surveillance infrastructures, which dampen and modulate behavioral variability, cannot hope to maintain a vibrant tradition of cultural and technical innovation. Efforts to repackage pervasive surveillance as innovation — under the moniker “Big Data” — are better understood as efforts to enshrine the methods and values of the modulated society at the heart of our system of knowledge production. The techniques of Big Data have important contributions to make to the scientific enterprise and to social welfare, but as engines of truth production about human subjects they deserve a long, hard second look.

#### Intellectual Exploration Occurs Only when Privacy is High

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf>

Intellectual-privacy theory explains why we should extend chilling effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed.90 Professor Timothy Macklem argues that “[t]he isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive.”91 A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling- effect doctrine’s normative commitment to err on the side of First Amendment values even if proof is imperfect.

#### Surveillance Corrodes Intellectual Freedom and Violates Civil Liberties

Richards, Neil. [Professor of Law, Washington University School of Law]. "THE DANGERS OF SURVEILLANCE," Harvard Law Review. vol. 126, pg. 1934 (2013),<http://www.harvardlawreview.org/media/pdf/vol126_richards.pdf>

Shadowy regimes of surveillance corrode the constitutional commitment to intellectual freedom that lies at the heart of most theories of political freedom in a democracy. Secret programs of wide-ranging intellectual surveillance that are devoid of public process and that cannot be justified in court are inconsistent with this commitment and illegitimate in a free society. My argument is not that intellectual surveillance should never be possible, but that when the state seeks to learn what people are reading, thinking, and saying privately, such scrutiny is a serious threat to civil liberties. Accordingly, meaningful legal process (that is, at least a warrant supported by probable cause) must be followed before the government can perform the digital equivalent of reading our diaries. But we must also remember that in modern societies, surveillance fails to respect the line between public and private actors. Intellectual privacy should be preserved against private actors as well as against the state. Federal prosecutions based on purely intellectual surveillance are thankfully rare, but the coercive effects of monitoring by our friends and acquaintances are much more common. We are constrained in our actions by peer pressure at least as much as by the state. Moreover, records collected by private parties can be sold to or subpoenaed by the government, which (as noted above) has shown a voracious interest in all kinds of personal information, particularly records related to the operation of the mind and political beliefs.95 Put simply, the problem of intellectual privacy transcends the public/private divide, and justifies additional legal protections on intellectual privacy and the right to read freely.96 Constitutional law and standing doctrine alone will not solve the threat of surveillance to intellectual freedom and privacy, but they are a good place to start.

## Impact on Immigration/Immigrants

#### NSA Surveillance Disproportionately Affects Immigrants

Conor Friedersdorf, “NSA Spying Has a Disproportionate Effect on Immigrants,” The Atlantic (Online), May 16, 2014. URL = <<http://www.theatlantic.com/politics/archive/2014/05/nsa-spying-> has-a-disparate-impact-on-the-privacy-rights-of-us-immigrants/371023/>

All I'd add is that the Obama administration's encroachments on the Fourth Amendment disparately affect naturalized citizens of the United States, almost all of whom still have friends or family members living in their countries of origin. When I call my parents, email my sister, or text my best friend, my private communications are theoretically protected by the Bill of Rights. In contrast, immigrants contacting loved ones often do so with the expectation that every word they say or write can be legally recorded and stored forever on a server somewhere. Xenophobia is one factor driving this double-standard. It does real harm to immigrants whose speech is chilled, as is clear to anyone who has made an effort to speak with them. Yet there has been little backlash against the Obama administration for affording zero constitutional protections to Americans engaged in speech with foreigners, and little sympathy for the innocent Americans, many of them immigrants, who are hurt by the approach Obama and many in Congress endorse.

## Legal Issues

#### NSA Surveillance Violates the Constitution

Peter M. Shane, [Chair in Law, Moritz College of Law, Ohio State University], "Foreword: The NSA And the Legal Regime for Foreign Intelligence Surveillance," A Journal of Law and Policy for the Information Society, 2014.

Professors Katherine Strandberg and Laura Donahue argue, however, that the programs Snowden revealed violate constitutional rights protections in other respects. In Membership Lists, Metadata, and Freedom of Association’s Specificity Requirement,138 Professor Strandberg argues that metadata surveillance is unconstitutional unless conducted in compliance with the First Amendment’s guarantee of freedom of association. As analyzed by Professor Strandburg, that right entails certain specificity requirements that the current Section 215 programs do not meet. In PRISM and the Interception of Communications Under Section 702 of the Foreign Intelligence Surveillance Act, 139 Professor Laura Donohue argues, Smith notwithstanding, the NSA’s Internet content surveillance program fails Fourth Amendment requirements. She agrees with Professor Yoo that the program is consistent with FISA, but argues that the program is unconstitutional because of the compulsory involvement of private telecom companies and the failure to prevent overbreadth. She concludes that the interception of all international communications fails the reasonableness test of Katz.

#### Even “Secret Courts” have found the NSA’s surveillance programs unconstitutional

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-> surveillance-violated-constitution-secret-fisa-court-found

Americans are being told that there’s no need to worry about the broad surveillance programs authorized by the controversial FISA Amendments Act of 2008. Yet a report from Wired this weekend paints a more disturbing picture: National Security Agency surveillance enabled by the FAA was found “unreasonable under the Fourth Amendment” by the secretive Foreign Intelligence Surveillance Court “on at least one occasion.” The court also found that the government’s implementation of its authority under the statute had “circumvented the spirit of the law.” Despite these troubling rulings from a court notorious for its deference to intelligence agencies, Congress is so unconcerned that lawmakers don’t even want to know how many citizens have been caught up in the NSA’s vast and growing databases.

#### The NSA Too Narrowly Defines Interception to Avoid Violating the 4th Amendment

Sanchez, Julian. [research fellow at the Cato Institute]. "NSA Surveillance Violated Constitution, Secret FISA Court Found," The CATO Institute. July 23, 2012, <http://www.cato.org/blog/nsa-> surveillance-violated-constitution-secret-fisa-court-found

Binney argues that when NSA officials have denied they are engaged in broad and indiscriminate “interception” of Americans’ communications, they are using that term “in a very narrow way,” analogous to the technical definition of “collection” above, not counting an e-mail or call as “intercepted” until it has been reviewed by human eyes. On this theory, the entire burden of satisfying the Fourth Amendment’s requirement of “reasonableness” is borne by the “minimization procedures” governing the use of the massive Pinwale database. On this theory, the constitutional “search” does not occur when all these billions of calls and emails are actually intercepted (in the ordinary sense) and recorded by the NSA, but only when the database is queried. This is a huge departure from what has traditionally been understood to be constitutionally permitted. We do not normally allow the government to indiscriminately make copies of everyone’s private correspondence, so long as they promise not to read it without a warrant: The copying itself is supposed to require a warrant, except in extraordinary circumstances. It appears almost certain that a very different rule is in effect now, at least for the NSA. It cannot be overemphasized how dangerous such a change would be. Traditionally, a citizen’s right to private communication was either respected or violated at the time it occurred: Your rights would be violated in realtime, or not at all, and even in the lawless era of J. Edgar Hoover, only so many citizens could be spied on at once. Under this new regime, the threat to our rights is perpetual. Even if this administration and the next are scrupulous about respecting civil liberties, even if every man and woman currently employed by the NSA is noble and pure of heart, the conversation you have today may well be there for the use or misuse of whoever holds power in ten years, or fifteen, or twenty. Will the incumbent president in 2032 resist the temptation to hunt for dirt in online chats from his opponent’s college years—showing greater restraint than so many past presidents? One must hope so—but better to design the rules of a free society so that such leaps of faith aren’t required.

#### The USFG has ruled that US Citizens have NO right to privacy when interacting with non-US individuals

Jameel Jaffer, “The official US position on the NSA is still unlimited eavesdropping power,”

Guardian (Online), May 14th, 2014. URL =

<http://www.theguardian.com/commentisfree/2014/may/14/nsa-eavesdropping-program- constitutional>

Modern American privacy law begins with Charles Katz, an accused gambler, making a call from a Los Angeles phone booth. In a now-famous opinion, Justice John Marshall Harlan concluded that the US Constitution protected Katz's "expectation of privacy" in his call. American phone booths are now a thing of the past, of course, and Americans' expectations of privacy seem to be fast disappearing, too. In two significant but almost-completely overlooked legal briefs filed last week, the US government defended the constitutionality of the Fisa Amendments Act, the controversial 2008 law that codified the Bush administration's warrantless-wiretapping program. That law permits the government to monitor Americans' international communications without first obtaining individualized court orders or establishing any suspicion of wrongdoing. It's hardly surprising that the government believes the 2008 law is constitutional – government officials advocated for its passage six years ago, and they have been vigorously defending the law ever since. Documents made public over the last eleven-and-a-half months by the Guardian and others show that the NSA has been using the law aggressively. What's surprising – even remarkable – is what the government says on the way to its conclusion. It says, in essence, that the Constitution is utterly indifferent to the NSA's large-scale surveillance of Americans' international telephone calls and emails:

The privacy rights of US persons in international communications are significantly diminished, if not completely eliminated, when those communications have been transmitted to or obtained from non-US persons located outside the United States.

That phrase – "if not completely eliminated" – is unusually revealing. Think of it as the Justice Department's twin to the NSA's "collect it all". The government filed the legal briefs last week in two criminal cases, one in Colorado and another in Oregon, in which the defendants are being prosecuted based on evidence acquired under the Fisa Amendments Act. Both defendants have sought to have the government's evidence suppressed on the grounds that the surveillance law is unconstitutional. (The ACLU joined with the defense team in the Colorado case to make that argument.) In support of the law, the government contends that Americans who make phone calls or send emails to people abroad have a diminished expectation of privacy because the people with whom they are communicating – non-Americans abroad, that is – are not protected by the Constitution. The government also argues that Americans' privacy rights are further diminished in this context because the NSA has a "paramount" interest in examining information that crosses international borders. And, apparently contemplating a kind of race to the bottom in global privacy rights, the government even argues that Americans can't reasonably expect that their international communications will be private from the NSA when the intelligence services of so many other countries – the government doesn't name them – might be monitoring those communications, too. The government's argument is not simply that the NSA has broad authority to monitor Americans' international communications. The US government is arguing that the NSA's authority is unlimited in this respect. If the government is right, nothing in the Constitution bars the NSA from monitoring a phone call between a journalist in New York City and his source in London. For that matter, nothing bars the NSA from monitoring every call and email between Americans in the United States and their non-American friends, relatives, and colleagues overseas. In the government's view, there is no need to ask whether the 2008 law violates Americans' privacy rights, because in this context Americans have no rights to be violated.

#### The NSA tracks every key-stroke

David Cole, [Hon. George Mitchell professor in law and public policy at Georgetown University Law Center and is the legal affairs correspondent for the Nation.], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

Other documents describe X-KEYSCORE, the NSA’s most powerful tool, which, as its name implies, enables the agency to track every keystroke on a computer, permitting the agency to monitor in real time all of a user’s e-mail, social-media and Web-browsing activity. In a single month in 2012, X-KEYSCORE collected 41 billion records for one NSA unit. Greenwald contends that this is the program Snowden was referring to when he said that, with an e-mail address, he could tap into any American’s communications. (The NSA has accused Snowden of exaggerating, but the documents suggest that he may be right.)

## Privacy

#### Surveillance is a Direct Assault on Privacy

Walter Simpson, [Contributor, Buffalo News], "The end of privacy? Government and private surveillance pose a growing threat to Americans," Buffalo News, May 10, 2013.

In contrast, surveillance is a direct assault on privacy. It attacks and eliminates privacy. Its chilling effect constrains and shrinks us through self-censorship of thought and action. When taken to the extreme, like in George Orwell’s “1984,” surveillance objectifies so thoroughly that it destroys our internal life. Our nation’s founders recognized the importance of privacy in the Bill of Rights. The Fourth Amendment to the U.S. Constitution states, “The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.” While this language is pre-9/11, Internet and cellphone, it speaks of the kind of nation the founders envisioned. In America, we have a constitutionally guaranteed right to a private life safe from unreasonable search and seizure. But our privacy is being eroded by leaps and bounds every day.

## Scope of NSA Surveillance

#### The NSA has too much information to process

David Cole, [Hon. George Mitchell professor in law and public policy at Georgetown University Law Center and is the legal affairs correspondent for the Nation.], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

Much has been written about the NSA’s omnivorous appetite for personal data — much of it by Greenwald for the Guardian and other outlets. In his new book, however, he offers a revealing and disturbing overview, illustrated by dozens of reproduced secret documents, of just how far the NSA has gone to achieve Alexander’s vision of collecting and knowing it all. Relying on newly disclosed and already disclosed documents, Greenwald shows that the scope of the NSA’s surveillance exceeds not only our imagination but also the agency’s capacity even to store, much less analyze, it all.

#### The NSA has exponentially increased the amount of information gathered daily since 2011

David Cole, [WP Contributor], "No Place to Hide by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All'," Washington Post, May 12, 2014.

In a one-month period last year, for example, a single unit of the NSA, the Global Access Operations unit, collected data on more than 97  billion e-mails and 124  billion phone calls from around the world; more than 3  billion of those calls and e-mails were collected as they passed

through the United States. As of 2012, the agency was processing more than 20 billion telecommunications per day. In a single month in 2011, the NSA collected 71 million calls and e- mails from Poland alone — not a major hub of terrorist activity, the last time I checked. The NSA has admitted that “it collects far more content than is routinely useful to analysts.” These numbers call to mind Sen. Everett Dirksen’s quip about government spending: “A billion here, a billion there, and pretty soon you’re talking about real money.”

## Soft Power

#### NSA Surveillance Paves the way for an Internet Authoritarian State and Erodes International Relations

Rid, Thomas. [PhD., Reader in War Studies at King's College London]. "The Rest of the Snowden Files Should Be Destroyed," Slate. September 10, 2013, http://www.slate.com/articles/technology/future\_tense/2013/09/nsa\_surveillance\_the\_rest\_of\_the

\_snowden\_files\_should\_be\_destroyed.html

Meanwhile, thirdly, authoritarian states get a confidence boost. “Washington ate the dirt this time,” wrote China’s Global Times, an outlet sometimes called the Fox News of China. The U.S. administration “has long been trying to play innocent victim of cyberattacks” but now turned out to be “the biggest villain,” said Xinhua, the state-run news agency. This argument, of course, is hypocrisy. The National Security Agency is not spying in order to round up Obama's political opposition, and Government Communications Headquarters is not listening to Internet traffic to help London's banks—both of which stand in sharp contrast to China's own practices.

Nevertheless, Snowden's revelations make it easier for the world's authoritarian regimes to crush dissent at home. A fourth result: Internet governance is creaking. Diminishing America and Britain’s diplomatic and moral standing is threatening the multistakeholder approach, so far a guarantor for a free and open Internet. A patchwork of smaller, sovereign "Internets" is becoming more and more likely. As a result, the Internet could now become more authoritarian, not less.

## Terrorism

#### There is no proof that surveillance prevents terror plots

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

There has been a lot of ominous stammering from Congress and the Obama administration about terrorist plots that have been disrupted by the programs. But thus far, only two concrete examples have been mentioned—not a great many for seven years of effort. First, there have been suggestions that the NSA programs helped apprehend an American who had done surveillance work for the terrorist gunmen in Mumbai, India, in 2008. His efforts, however, were of limited importance to the event, and his eventual arrest didn’t prevent the attack. The second was the 2009 Zazi case, in which three Afghan-Americans trained in Pakistan before returning to the United States and plotted to set off bombs in the New York subway system. Given the perpetrators’ limited capacities, it is questionable whether the plot would ever have succeeded.

Furthermore, the plot was disrupted not by NSA data-dredgers but by standard surveillance: British intelligence provided a hot tip about Zazi based on e-mail traffic to a known terrorist address—one that had long been watched. At that point, U.S. authorities had good reason to put the plotters on their radar. Having NSA’s megadata collection may have been helpful, but it seems scarcely to have been required. Actually, it is not clear that even the tip was necessary because the plotters foolishly called attention to themselves by using stolen credit cards to purchase large quantities of potential bomb material.

#### Policing foils more terror plots than NSA surveillance

John Mueller [political scientist at Ohio state] and Mark G. Stewart [civil engineer at the University of Newcastle in Australia], "Three Questions about NSA Surveillance," Cato Institute, June 13, 2013.

A set of case studies of the 53 post-9/11 plots by Islamist terrorists to damage targets in the United States suggests this is typical. Where the plots have been disrupted, as in the Zazi case, the task was accomplished by ordinary policing. The NSA programs scarcely come up at all. When asked on Wednesday if the NSA’s data-gathering programs had been “critical” or “crucial” to disrupting terrorist threats, the agency’s head testified that in “dozens” of instances the database “helped” or was “contributing”—though he did seem to agree with the word “critical” at one point. He has promised to provide a list of those instances. The key issue for evaluating the programs, given their privacy implications, will be to determine not whether the huge database was helpful but whether it was necessary.

#### Data Mining Does not Work for Terrorism because every plot is unique

Jim Harper, [director of information policy studies at the Cato Institute], "Officials Need to Come Clean on NSA Surveillance Activities," Cato Institute, June 6, 2013.

Data mining works with credit card fraud. There are thousands of examples per year from which to build models of what credit card fraud looks like in data. And the cost of getting it wrong is low. Credit card companies may call a customer or cause them a modest inconvenience by cancelling a card. Data mining won’t work for terrorism because terrorism is too rare. There aren’t patterns reflecting terrorism planning or execution. Each plan and each attack, successful or unsuccessful, has been very different from the others. And the cost of false positives is high. Law enforcement personnel waste their time chasing false leads. Wrongly accused people are investigated, questioned, placed on no-fly lists or other derogatory lists, and sometimes people are wrongly arrested.

#### NSA Surveillance only works overseas, there is no reason to use it in the United States

Erik J. Dahl, [Assistant Professor of National Security Affairs at the Naval Postgraduate School in Monterey, California], "Discussion Point: It's not Big Data, but Little Data, that Prevents Terrorist Attacks" National Consortium for the Study of Terrorism and Responses to Terrorism, July 25, 2013. http://www.start.umd.edu/news/discussion-point-its-not-big-data-little-data-prevents-terrorist-attacks

But another one of our findings is that the most effective tools in preventing terrorist attacks are relatively simple, old fashioned police methods, such as the use of undercover officers, informants, and tips from the public. This is especially true for domestic plots and attacks: of the 109 failed plots within the United States since 9/11, more than 75 percent were foiled at least in part because of traditional law enforcement methods, and not—from what we can gather—from NSA surveillance. Thus it is not surprising that government officials have said most of the 50 or so plots that have been foiled by the NSA monitoring programs were overseas3. In other countries we can’t necessarily rely on local authorities, and spying—whether conducted by the NSA or the CIA—is a critical tool for our national security. But here in the U.S., the most important terrorism¶ prevention tool remains the country’s 800,000 police officers, deputy sheriffs, and other local law enforcement officials,¶ supported by members of the public who "see something and say something," calling authorities when something doesn’t¶ look right.

#### There was information on the 9/11 attack before it happened but the plot was not prevented

Jaffer, Jameel. [Fellow at the Open Society Foundations and deputy legal director of the American Civil Liberties Union]. "Needles Are Harder to Find in Bigger Haysticks," The New York Times. June 10, 2013, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-> surveillance-threat-real-or-imagined

It’s also worth remembering that the intelligence community’s biggest challenge has never been collecting information; the biggest challenge has always been making sense of it. Launching new programs to collect more information can be a good way to pad the pockets of defense contractors and data-miners, but, as many have noted, it isn’t usually a good way to identify terrorist threats. The analogy is now a bit threadbare, but it’s still useful: You don’t find needles by building bigger haystacks. After the NSA launched the warrantless wiretapping program, FBI agents repeatedly complained that they were drowning in useless information. (Eric Lichtblau wrote: “The torrent of tips led [the FBI] to few potential terrorists inside the country they did not know of from other sources and diverted agents from counterterrorism work they viewed as more productive.”). One of the 9/11 Commission’s most important observations was that the intelligence community had information in the summer of 2001 that could have allowed it to prevent the 9/11 attacks. The problem wasn’t that it lacked information, but that it didn’t understand the information it had. Finally, “effectiveness” isn’t as simple as you make it out to be. A program can be effective in some very narrow sense but also seriously compromise our democracy over the long term. A program can be effective in some very narrow sense but also be fundamentally inconsistent with our values. Again, I agree that the effectiveness question is worth asking. But answering the effectiveness question isn’t as simple as asking whether these surveillance programs yielded useful information.

#### Terrorists are adapting to circumvent surveillance

Dozier, Kimberly. [staff writer at the Associated Press]. "AL-QAIDA SAID TO BE CHANGING ITS WAYS AFTER LEAKS," The Associated Press. July 26, 2013, http://bigstory.ap.org/article/al- qaida-said-be-changing-its-ways-after-leaks

Two U.S. intelligence officials say members of virtually every terrorist group, including core al- Qaida members, are attempting to change how they communicate, based on what they are reading in the media, to hide from U.S. surveillance. It is the first time intelligence officials have described which groups are reacting to the leaks. The officials spoke anonymously because they were not authorized to speak about the intelligence matters publicly. The officials wouldn't go into details on how they know this, whether it's terrorists switching email accounts or cellphone providers or adopting new encryption techniques, but a lawmaker briefed on the matter said al- Qaida's Yemeni offshoot, al-Qaida in the Arabian Peninsula, has been among the first to alter how it reaches out to its operatives. The lawmaker spoke anonymously because he would not, by name, discuss the confidential briefing. Shortly after Edward Snowden leaked documents about the secret NSA surveillance programs, chat rooms and websites used by like-minded extremists and would-be recruits advised users how to avoid NSA detection, from telling them not to use their real phone numbers to recommending specific online software programs to keep spies from tracking their computers' physical locations.